

PROBABILISTIC SIGNATURE SCHEME

ABSTRACT OF THE DISCLOSURE

5 An RSA-based signing scheme that combines essentially
optimal efficiency with attractive security properties. One
preferred signing routine requires one RSA decryption plus some
hashing, verifications requires one RSA encryption plus some
hashing, and the size of the signature preferably is the size of
10 the modulus. Given an ideal underlying hash function, the scheme
is not only provably secure, but has security tightly related to
the security of RSA. An alternative embodiment maintains all of
the above features and, in addition, provides message recovery.
The techniques can be extended to provide schemes for Rabin-based
15 signatures or signatures using other trapdoor functions.